Krüpteerimine ei tähenda privaatsust: mida metaandmed teie kohta ütlevad

Krüpteeritud sisu ja nähtavad metaandmed on kaks eri asja. Kui teenus räägib "ots-otsani krüpteerimisest", räägib ta ainult poole loost.

Lukk, mis ei kaitse kõike

Suur osa tänapäevastest sõnumside teenustest reklaamib ots-otsani krüpteerimist. Ja see on tõsi: sõnumite sisu liigub krüpteeritult, nii et keegi teel – isegi mitte teenusepakkuja – ei saa teksti edastamise ajal lugeda. Seni on väide täpne.

Probleem on selles, et sisu on vaid osa loost. Isegi kui keegi ei saa lugeda, mida te ütlete, teab teenus muid asju väga suure täpsusega: kellega te räägite, mis kell, kui sageli, millisest ligikaudsest asukohast, millisel seadmel, kui palju sõnumeid saadate ja kui palju vastu võtate, kui palju faile jagate. Seda kõike nimetatakse metaandmeteks. Ja metaandmed räägivad paljudel juhtudel peaaegu sama palju kui sõnum ise.

Mida metaandmed paljastavad

Paljude asjade teadmiseks pole vaja sõnumit lugeda. Kui inimene helistab või kirjutab onkoloogile kuue kuu jooksul igal teisipäeva hommikul kell üheksa, pole vaja vestlust kuulda, et aimata, mis toimub. Kui kaks inimest vahetavad päevas sada sõnumit ja lõpetavad selle järsku, pole vaja lugeda ühtegi, et mõista, mis on juhtunud. Kui maksunõustaja saab kvartali lõpetamisele eelneval õhtul samalt kliendilt kakskümmend sõnumit järjest, räägib muster iseenda eest.

Metaandmed paljastavad käitumismustreid: kes on kellega suhtes, millised on iga inimese ajakavad, millal nad on ärvel, millal magavad, millal reisivad, millised kliendid on kõige aktiivsemad, millised ametisuhted on kõige intensiivsemad. Metaandmeid koguv server saab luua üksikasjaliku profiili iga kasutaja isiklikust ja ametialasest elust, ilma et oleks kordagi lugenud ühtegi sõna sellest, mida ta kirjutab.

On olemas ajalooline näide, mis illustreerib seda karmilt. NSA endine direktor Michael Hayden sõnastas selle 2014. aastal otsekoheselt: *"We kill people based on metadata"*. Väide viitas USA sõjalistele operatsioonidele sihtmärkide vastu, mis tuvastati üksnes nende suhtlusmustrite põhjal. Mitte ühtegi loetud sõnumit. Ainult kontaktigraaf ja ajakavad.

See, et teenus kogub metaandmeid, ei tähenda tingimata, et ta kasutab neid oma kasutajate vastu. See tähendab, et tal on selleks võimekus ja et kolmandal osapoolel, kellel on juurdepääs nendele andmetele – kohtumääruse, turvarikkumise või müügi kaudu kolmandatele isikutele, kui teenusetingimused seda lubavad –, on see samuti olemas.

Juurdepääs kontaktiraamatule

Teine vektor, mis jääb peaaegu märkamatuks: kontaktide nimekiri. Suur osa sõnumside teenustest küsib registreerumisel juurdepääsu telefoni kontaktiraamatule. Nad laadivad kõik numbrid oma serverisse, et näidata, kes veel teenust kasutab. Sellest hetkest on ettevõttel täielik kaart kasutaja suhetest, isegi kui ta pole kunagi kellelegi ühtegi sõnumit kirjutanud.

Ametisaladuse hoidjale – advokaadile, arstile, psühholoogile, nõustajale – sisaldab see kontaktiraamat kliente. Kui kontaktiraamat on laaditud kolmanda osapoole serverisse, asuvad klientide nimed infrastruktuuris, mille jurisdiktsiooni ja poliitikaid professionaal ei kontrolli. Ametisaladust ei murta vestluse lekkimise päeval: see murti palju varem, laadimise nõustumise hetkel.

Erinevus krüpteerimise ja mittekogumise vahel

Krüpteerimine on sisu kaitsmine. Privaatne olemine on see, et ei koguta seda, mida pole vaja. Need on eri asjad ja erinevus on operatiivselt kriitiline. Teenus saab kõik sõnumid täiuslikult krüpteerida ja samal ajal teada metaandmete kaudu oma kasutajate kohta peaaegu kõike. Need kaks on täiesti ühilduvad. Tegelikult on see sektori valdav ärimudel.

Õige küsimus teenuse tegeliku privaatsuse hindamiseks ei ole *"kas see krüpteerib sisu?"*. Sellele küsimusele on vastatud aastaid. Õige küsimus on: *"milliseid metaandmeid see genereerib ja kus neid hoitakse?"*. Ja eelkõige: *"milliseid metaandmeid tal pole vaja genereerida?"*.

Arhitektuur, mis minimeerib metaandmeid disaini kaudu – mitte lubaduse, mitte sisepoliitika kaudu –, on struktuurselt privaatsem kui arhitektuur, mis neid kogub ja krüpteerib. Sest andmeid, mida pole olemas, ei saa lekitada, müüa, kohtumäärusele üle anda ega turvarikkumise käigus kaotada.

Professionaalsele lugejale

Kui teie ametitegevus hõlmab saladust, konfidentsiaalsust või lihtsalt austust kolmandate isikute teabe vastu, tasub küsimused esitada selles järjekorras:

1. Kas rakendus, mida suhtluseks kasutan, krüpteerib sisu? (Tõenäoliselt jah.)
2. Kas see krüpteerib metaandmed? (Tõenäoliselt mitte.)
3. Kas see genereerib metaandmeid, mida ta toimimiseks *ei vaja*? (Peaaegu kindlasti jah.)
4. Kus neid metaandmeid hoitakse ja millise jurisdiktsiooni all? (Tõenäoliselt väljaspool Euroopa Majanduspiirkonda.)
5. Kas mu klient või patsient teab, et tema andmed on seal?

Viimane küsimus on ebamugav. Sest aus vastus on enamikul juhtudel: ei.

See artikkel on esimene sarjast professionaalsete suhtlusvahendite tegelikust toimimisest. Järgmised väljaanded käsitlevad GDPR-i järgimist sõnumsides ja ametisaladuse kontseptsiooni digiajastul.

Allikad ja täiendav lugemine

- Hayden, M. – Deklaratsioon Johns Hopkinsi ülikoolis, 2014 ("We kill people based on metadata"). Avalikud transkriptsioonid saadaval.
- GDPR (EL määrus 2016/679), art 4 ja 5 – isikuandmete määratlus ja töötlemise põhimõtted (metaandmed on isikuandmed).
- Euroopa Andmekaitseinspektor ja EDPB – arvamused liiklusandmete ja metaandmete töötlemise kohta elektroonilises sides (e-privaatsuse direktiiv).

← EelmineLühike lakipitseri ajaluguJärgmine →Ametisaladus digiajastul

Viimased lugemised

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Võtke see artikkel endaga kaasa kuhu iganes vaja.

↓ Markdown ↓ Lihttekst ↓ PDF

Fail laaditakse alla teie seadmesse. Sealt saate selle salvestada, importida Solo2-sse või jagada kus iganes soovite. Cuadernos ei otsusta sihtkohta teie eest.

Lakipitsat · SHA-256 3abf3d4c09e3b2e672552c7378e83d26b540231b6667c0f679a04ab277e8e739

Cuadernos Lacre · Ettevõtte Menzuri Gestión S.L. väljaanne ·
kirjutanud R.Eugenio · toimetanud Solo2 meeskond.